IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
BALTIMORE DIVISION

JASON ALFORD *et al.*,

Plaintiffs,

v.

THE NFL PLAYER DISABILITY & SURVIVOR BENEFIT PLAN *et al.*,

Defendants.

Case No. 1:23-cv-00358-JRR

ORDER GOVERNING PRODUCTION OF
ELECTRONICALLY STORED INFORMATION AND DOCUMENTS

The undersigned counsel for Defendants and Plaintiffs (individually a "Party" and collectively the "Parties") in the above-captioned Action (the "Action"), agree that the following Order governs the discovery and production of Electronically Stored Information ("ESI"), and Documents in this Action unless the Parties agree in advance and in writing or if this Order is modified by the Court. The purpose of this Order is to facilitate the timely production of ESI and Documents in an efficient manner and in accordance with the Federal Rules of Civil Procedure and to promote the avoidance or early resolution of disputes regarding the discovery of ESI and Documents and to promote the avoidance or early resolution of disputes regarding the discovery of ESI without Court intervention. By stipulating to this Order and agreeing to produce ESI or Documents in a particular form or forms, no Party waives any objections to producing any particular document or category of documents on any grounds. Except as specifically set forth herein, this Order does not: (a) alter or affect the applicability of the Federal Rules of Civil

Procedure ("Federal Rules") or any Local Rules of the U.S. District Courts ("Local Rules"), as applicable; (b) address, limit, determine, or affect the relevance, discoverability, or admissibility as evidence of any ESI or Document; or (c) alter or affect the objections to discovery available under the Federal Rules. Therefore, the Parties have stipulated to the following negotiated terms, subject to the Court's approval, and the Court hereby **ORDERS** that the following shall govern the discovery and production of ESI and Documents in this Action.

1. COOPERATION

The Parties are aware the Court expects cooperation on issues relating to the identification, preservation, collection, search, review, production, integrity, and authentication of ESI. The parties commit to work in good faith throughout the matter consistent with this Court's Principles for the Discovery of Electronically Stored Information in Civil Cases ("Principles for Discovery of ESI").

2. ESI LIAISONS

To promote transparency, communications, and cooperation between the Parties and to help ensure that any disputes regarding ESI that the parties are unable to resolve are presented to the Court at the earliest reasonable opportunity, the Parties shall designate e-discovery liaisons for purposes of meeting and conferring on ESI topics. As proposed by the Parties, the co-ESI liaisons for Plaintiffs shall be Ben Barnett of Seeger Weiss LLP and D. Nicole Guntner of Aylstock, Witkin, Kreis, Overholtz, PLLC, and the ESI liaison for Defendants shall be Jonathan Le of O'Melveny & Myers LLP. All productions of ESI by any Party or non-Party shall be sent to the Parties' respective ESI liaison and lead counsel, and any identified designees.

3. CONTINUING OBLIGATIONS.

The Parties will continue to meet and confer regarding any issues as necessary and

appropriate. This Protocol does not address or resolve any objections to the scope of the Parties' respective discovery requests. The Parties agree that e-discovery will be conducted in phases, and the Parties will meet and confer regarding discovery of data sources not listed herein.

4. RESERVATION OF RIGHTS.

The Parties retain the right, upon reviewing any productions made by another Party in this Action or conducting other investigation and discovery, to request that Documents from additional non-custodial data sources and custodians be produced. The Parties shall meet and confer regarding such request(s) prior to any search or production related thereto.

5. DEFINITIONS

a. "**Confidentiality Designation**" means the legend affixed to "Confidential" Discovery Material as defined by, and subject to, the terms of the Stipulated Protective Order entered in this Action.

b. "**Defendants**" means and refers to the named Defendants in the above-captioned matter, as well as any later-added Defendants, as well as their directors, principals, employees, agents, and affiliates.

c. "**Document**" is defined to be synonymous in meaning and equal in scope to the usage of this term in Federal Rules of Civil Procedure 26 and 34. The term "Document" shall include Hard Copy Documents, Electronic Documents, and ESI as defined herein.

d. "**Extracted Full Text**" means the full text that is extracted electronically from native electronic files, and includes all header, footer, and document body information.

e. "**Electronically Stored Information**" or "**ESI**," as used herein has the same meaning as in the Federal Rules of Civil Procedure 26 and 34.

f. "**Hard-Copy Document**" means Documents existing in tangible form, including but

not limited to paper Documents.

g. "**Hash Value**" is a unique numerical identifier that can be assigned to a file, a group of files, or a portion of a file, based on a standard mathematical algorithm applied to the characteristics of the data set.

h. "**Load Files**" means electronic files provided with a production set of documents and images used to load that production set into a receiving Party's document review platform and correlate its data within that platform.

i. "**Media**" means an object or device, real or virtual, including but not limited to a disc, tape, computer, or other device on which data is or was stored.

j. "**Metadata**" (i) structured, i.e., fielded, information embedded in a Native file which describes, inter alia, the characteristics, origins, usage, and/or validity of the electronic file; (ii) information generated automatically by the operation of a computer or other information technology system when a Native file is created, modified, transmitted, deleted, or otherwise manipulated by a user of such system; (iii) information, such as Bates numbers, created during the course of processing documents or ESI for production; and (iv) information collected during the course of collecting documents or ESI, such as the name of the Media device, or the custodian or non-custodial data source from which it was collected.

k. "**Native"** means and refers to a Document's associated file structure defined by the original creating application. For example, the native format of an Excel workbook is a .xls or .xslx file.

l. "**Optical Character Recognition**" or "**OCR**" means the process of recognizing and creating a file containing visible text within an image.

m. "**Searchable Text**" means the Native text extracted from ESI and any OCR text generated from a Document or electronic image.

n. "**And**" and "**or**" shall be construed conjunctively or disjunctively as necessary to make their use inclusive rather than exclusive, e.g., "and" shall be construed to mean "and/or".

o. "**Include**" and "**including**" shall be construed to mean "include, but not be limited to" and "including, but not limited to."

p. Reference to the singular shall also be deemed to refer to the plural, and vice-versa.

q. "**Responsive**," "**Relevant,**" and "**Discoverable**" are used interchangeably, and each shall be construed to encompass the broadest possible scope.

6. IDENTIFICATION OF ESI/SEARCH METHODOLOGY

Within a reasonable time following service of written requests for production ("RFPs"), in order to facilitate discussions on the potential application of search terms, technology-assisted review ("TAR"), or other filtering search and culling technologies, each party shall provide in writing a list of custodians or data sources within that party's control that will be searched for potentially relevant Documents and ESI in response to the RFPs.

7. SEARCH

The Parties must meet and confer to address the method(s) the Parties will use relating to the collection and production of relevant documents. The Parties recognize and agree that they may use one or more search methodologies to identify, cull, review, and produce relevant, non-privileged ESI and Documents. The Parties, therefore, agree to cooperate in good faith regarding the disclosure and formulation of appropriate search methodology. The Parties must disclose and discuss any proposed use of software or other technologies used to identify or eliminate sources

of potentially relevant documents, including keyword or Boolean searching, file-type culling, date-range culling, de-duplication, filtering, near de-duplication, email thread suppression, clustering, concept searching, or other TAR.

If a producing party plans to use electronic search terms to cull ESI and Documents, the Parties will meet and confer regarding the terms and any other culling parameters to be applied to the searches, such as date ranges. Upon request, the Parties agree to provide a list of relevant internal terminology, including potentially relevant project and code names, code words, acronyms, abbreviations, and nicknames, if any, following a reasonable inquiry. As part of that process, the producing party will disclose information regarding the search platform to be used, including terms and connectors appropriate to the platform, as well as any other search parameters. After receiving this information, the receiving party may propose changes to the search terms and parameters. If a producing party does not accept this proposal or the receiving party believes that additional or different terms or parameters beyond those initially offered by a producing party are appropriate, the Parties shall participate in an iterative and cooperative meet and confer process to negotiate reasonable and appropriate methods.

After the Parties have agreed upon collection and identification methods, and only if a Party believes in good faith that use of the disclosed methods would result in deficiencies in production, the Parties will work collaboratively on any revisions to such methods, on the understanding that this may be an iterative process. If there are any issues that cannot be resolved regarding search and retrieval methods, the Parties shall bring any disputes to the attention of the Court.

Nothing in this section shall limit a Party's right to seek agreement from the other Parties or a court ruling to modify previously agreed-upon collection and identification methodology.

The fact that ESI has been identified in an agreed-upon collection and identification method shall not prevent any Party, after attorney review on a good-faith basis, from withholding such file from production on the grounds that the file is not relevant, that it is protected from disclosure by applicable privilege or immunity, or that it is governed by any applicable privacy law or regulation.

8. KNOWN RELEVANT MATERIAL MUST BE PRODUCED

Notwithstanding any agreement to collect and produce ESI and Documents under this Order, the Parties will produce non-privileged, non-objectionable Documents actually known to the Parties' Counsel to be relevant to the claims or defenses in this matter, regardless of whether or not such Documents are identified for review using search terms, TAR, or any other culling, search, or review methodologies. Privileged documents may be withheld from production provided they are listed in a privilege log consistent with the requirements of this Protocol.

9. DISCRETE DOCUMENT COLLECTIONS

Discrete document collections, such as, by way of example only, folders of relevant ESI or Documents specifically created or segregated by Plaintiffs, Defendants, or Defendants' employees, before or after the commencement of this litigation, shall be reviewed for relevancy in their entirety without regard to whether each file or Document in the collection is responsive to a search term or otherwise flagged as potentially relevant by another search or review technique or methodology. Following that review, relevant documents shall be produced consistent with this Protocol. Privileged documents may be withheld from production provided they are listed in a privilege log consistent with Section 17 of this Protocol. If during the course of discovery a Receiving Party believes that it has identified an additional relevant "discrete document collection" the Parties shall meet and confer regarding the review and production of the newly identified discrete document collection.

10. INACCESSIBLE DOCUMENTS

If a Producing Party believes potentially relevant ESI or Documents are not reasonably accessible, the Producing Party will provide sufficient information about the ESI and Documents (and their custodial or non-custodial sources) to enable the Parties to confer in good faith about whether such ESI and Documents need to be collected, reviewed, and produced.

11. FORMAT FOR PRODUCTIONS

The following section governs the format of productions of ESI and Documents by the Parties and shall apply to all discovery of ESI and Documents by the Parties in this case, unless the Parties agree in advance and in writing or if this Order is modified by the Court.

a. Production in Reasonably Usable Form.

The Parties shall produce all ESI and Documents in a reasonably usable form.

b. File Types and Formats.

All spreadsheet (*e.g.*, Microsoft Excel, Corel Quattro, etc.), files shall be produced as native files with TIFF placeholder images. All word processing (*e.g.,* Microsoft Word), presentation (*e.g.*, Microsoft PowerPoint), PDF, and Media (*e.g.*, audio and video) files shall be produced as Native files with TIFF placeholder images where reasonably possible, unless redactions are required, in which case subsection below shall apply. Emails shall be produced as TIFF images. Documents containing color need not be produced in color in the first instance. However, the receiving party may, in good faith, request production of such documents in color by providing a list of the Bates numbers of documents it requests to be produced in color format. The producing Party shall not unreasonably deny such requests.

c. Native Files.

Any Document produced in Native Format shall be given a file name consisting of a unique

Bates number and, as applicable, a Confidentiality Designation; for example, "ABC00000002_Confidential." For each Native File produced, the production will include a *.tiff image slipsheet indicating the production number of the Native File and the Confidentiality Designation and stating, "File Provided Natively." To the extent that it is available, the original Document text shall be provided in a Document- level multi-page UTF-8 with BOM text file with a text path provided in the *.dat file. Otherwise the text contained on the slipsheet language shall be provided in the *.txt file with the text path provided in the *.dat file. Native Files will be produced in a separate folder on the production Media.

d. TIFF Images.

All ESI and Documents not otherwise specified in Section 11(b) of this Order shall be produced as single-page, Group IV TIFF with a resolution of 300 DPI, in a manner that does not degrade the original image. Any Document produced as TIFF images shall be named according to the Bates number of the corresponding TIFF image. Bates numbers shall be endorsed on the lower right corner of all TIFF images. Each *.tiff file should be assigned a unique name matching the Bates number of the corresponding image. All TIFF images should be provided in single-page, Group IV TIFF with a resolution of 300 DPI. To the extent possible, original orientation will be maintained (*i.e.*, portrait-to-portrait and landscape-to-landscape). TIFFs shall convey the same information and image as the original Document, including all commenting, tracked changes, hidden text, and formatting that is visible in the Document's native application. All hidden content will be expanded, extracted, and rendered in the TIFF file and to the extent possible, Bates numbers and Confidentiality Designations should be electronically branded on each produced *.tiff image. These *.tiff images should be provided in a separate folder, and the number of TIFF files per folder should be limited to 2,000 files unless necessary to prevent a file from splitting across folders. A

receiving Party may make a good faith request that a Document originally produced in TIFF pursuant to this section be produced in native. The Producing Party shall not unreasonably deny such requests.

e. File Text.

Except when a file's full text cannot be extracted (*e.g.*, when a file is being redacted under an assertion of privilege), the full text will be provided in the format of a single *.txt file for each file (*i.e.*, not one *.txt file per *.tif image). When ESI contains text that cannot be extracted, the available *.tif image will be OCR'd or, as applicable, the redacted Native file will have its text re-extracted, and file-level text will be provided. Searchable Text will be produced as single file UTF-8 text files with the text file named to match the beginning production number of the file. The full path of the text file must be provided in the *.dat data Load File.

f. Compressed Files.

Compressed file types (i.e., CAB., GZ., TAR., .Z., ZIP) shall be decompressed in a reiterative manner to ensure that a zip within a zip is decompressed into the lowest possible compression resulting in individual files.

g. Databases, Document Management Systems, Collaboration Tools or Software, and Structured, Aggregated or Application Data.

The Parties will meet and confer to address the production and production format of any relevant data contained in databases, document management systems, collaboration tools or software, and structured, aggregated, or application software during the parties' Rule 26(f) conference and any additional meet-and-confer necessary to ensure conformity with Principle 1.02 of Principles for Discovery of ESI (Cooperation and Exchange of Information). The Parties will reasonably cooperate in the exchange of information concerning such databases to facilitate

discussions on productions and production format. If the Parties cannot reach agreement, the matter will be submitted to the Court or its designee.

h. Hard Copy Documents

Documents that exist in Hard Copy will be scanned to *.tiff image format as set forth in Subsection I(d) above. In scanning and producing Hard Copy Documents:

1. OCR should be performed on a document level and provided in document-level *.txt files named to match the production number of the first page of the document to which the OCR text corresponds. OCR text should not be delivered in the data load file or any other delimited text file. OCR software must be set to the highest quality setting for any previously-unscanned paper documents, and reasonable quality control measures shall be used to ensure that the integrity of scanned copies of previously unscanned paper documents are preserved for OCR (*e.g.*, pages are not angled or skewed, text is not blurred or obscured, etc.). Settings such as "auto-deskewing" and "autorotation" must be turned on during the OCR process to maximize text recognition on any given page. Documents containing foreign language text must be OCR'ed using the appropriate settings for that language (*e.g.*, OCR of German documents must use settings that properly capture umlauts).

2. Hard Copy Documents that are not text-searchable shall be made searchable by OCR prior to production where possible.

3. The Parties will use best efforts to unitize the Hard Copy Documents correctly. In scanning paper documents, distinct documents should not be merged into a single record, and single documents should not be split into multiple records. Scans should maintain document relationships, i.e., attachment status.

4. Documents are to be produced as they were kept in the ordinary course of business. For Documents found in folders or other containers with labels, tabs, indexes, or other identifying information, such indexes, labels, and tabs shall be scanned. Pages with Post-It notes shall be scanned both with and without the Post-It, with the image of the page with the Post-It preceding the image of the page without the Post-It. In the case of an organized compilation of separate Documents (for example, a binder containing several separate Documents behind numbered tabs), the Document behind each tab should be scanned separately, but the relationship among the Documents in the compilation should be reflected in the proper coding of the beginning and ending document and attachment fields.

i. System Files

Common system files and application executable files will be filtered out using the national software reference library ("NSRL") NIST hash set list. Additional culling of file types based on file header information may be applied to the following, provided these files are not known to be otherwise attached, embedded in, or included with an otherwise relevant Document, or are not themselves reasonably known to contain information relevant or contain relevant data or are used to interface with users or interact with or access individual or aggregated user data: Application Package File, Backup Files, Batch Files, Binary Disc Image, C++ File Formats, Cascading Style Sheet, Configuration File, Database File, Dictionary Files, Dynamic Link Library, Event Log Files, Executable Files, Hypertext Cascading Stylesheet, Java Archive Files, JavaScript Files, JavaScript Source Code and Class Files, Macintosh Resource Fork Files, Package Manager Files, Program Files, Program Installers, Python Script Files, Shell Script Files, System or Temporary Files, Thumbnail Cache Files, Troff Files, Truetype Font Files, Windows Cabinet File, Windows Command Files, Windows File Shortcut, Windows Help Files, Windows Metafiles and Enhanced

Metafiles, Windows Spool Files, Windows System File.

j. De-duplication

The Parties shall use best efforts to de-duplicate ESI globally (i.e., within a particular custodian's files, and across all custodial and non-custodial sources). Documents and family groups are considered exact duplicates if they have a matching MD5 or SHA-1 Hash Value as compared against the same document type (i.e., family group or stand-alone file). Hash Values of emails will be calculated on the concatenated values of at least the following fields: From, To, CC, BCC, Subject, Date Sent, Time Sent, Attachment Names, Body, and the Hash Values of all attachments. The names of all custodians and non-custodial sources who were in possession of a Document prior to de-duplication will be populated in the ALL CUSTODIANS metadata field. The original file paths of a Document prior to de-duplication will be populated in the ALL FILE PATHS[1] metadata field. Near-duplicate Documents shall be produced.

If the Parties make supplemental productions following an initial production, the Parties shall also provide each supplemental production an overlay file to allow the Receiving Party to update the ALL CUSTODIANS field. The overlay file shall include both all custodians listed in the ALL CUSTODIANS field in prior productions and any custodians newly identified in the current supplemental production.

[1] ALL FILE PATHS metadata field shall include the original file/folder paths, including file name for non-emails, where reasonably available, of all the locations where copies of the item were located at the time of collection, separated by semi-colons. For emails collected from container files (*e.g.*, .pst), these include the original file paths of the container files and the location of the emails within the folder structure of the mail container/.pst from which it was collected, where reasonably available.

k. Embedded Files.

Embedded files or objects, except for images embedded in emails, are to be produced as family groups. Embedded files shall be extracted as separate files and shall be produced as attachments to the file in which they were embedded. Embedded files should be assigned Bates numbers that directly follow the Bates numbers on the Documents within which they are embedded.

l. Parent-Child Relationships.

All family relationships should be preserved, and all attachments should sequentially follow the parent Document.

m. Hyperlinks

Document(s) and/or folder(s) of documents that are hyperlinked inside a responsive document (including hyperlinks inside emails or messages) within a Producing Party's custody, possession, or control do not need to be produced in the first instance as part of the same family group as the Document containing the hyperlink. The Requesting Party may submit a list of hyperlinks to the Producing Party and request that they be searched for by identifying the Bates number and URL or link text for each requested link. The Producing Party shall conduct a reasonable search to locate the contemporaneous or nearest in time version of the hyperlinked document at that location. The Producing Party will produce any relevant documents, log any privileged documents, and identify by Bates number any previously produced documents. If the contemporaneous or nearest in time version of the hyperlinked document is no longer available, the Producing Party shall inform the Requesting Party and produce a reasonable number of other existing versions of the document closest in time to when the hyperlink was created or sent.

n. Dynamic Fields.

Documents with dynamic fields for file names, dates, and times will be processed to show the field code (*e.g.*, "[FILENAME]" or [AUTODATE]) rather than the values for such fields existing at the time the file is processed.

o. Time Zone.

All provided metadata pertaining to dates and times will be standardized to UTC.

p. Bates Numbering.

Bates numbering should be consistent across the production, contain no special characters, and be numerically sequential within a given Document. If a Bates number or set of Bates numbers is skipped, the skipped number or set of numbers should be noted with a placeholder. Attachments to Documents will be assigned Bates numbers that directly follow the Bates numbers on the Documents to which they were attached. In addition, wherever possible, each *.tiff image will have its assigned Bates number electronically "burned" onto the image.

q. Excluded File Types.

Absent a particularized need and good cause showing, the Parties agree that there is no need to collect ESI from the following sources:

1. Deleted, slack, fragmented, or other data accessible only by forensics;
2. Random access memory (RAM), temporary files, or other data difficult to preserve without disabling the operating system;
3. On-line access data such as temporary internet files, history, cache, and cookies; and
4. Back-up data files that are maintained in the normal course of business for purposes of disaster recovery, including (but not limited to) backup tapes, disks, SAN, and other forms of Media, and that are duplicative of data more accessible elsewhere.

r. Email Threading

The Parties agree that the Producing Party may, at its discretion, elect to review only the most inclusive email thread in determining the relevancy of the prior or lesser-included emails or for any other non-production purpose. Production of a most inclusive email thread does not relieve the Producing Party of its obligation to produce relevant prior or lesser-included emails. No Document shall be withheld from production on the basis that it is included in a produced more-inclusive email.

s. Redactions.

Other than as permitted by this Order or the Stipulated Protective Order entered in this litigation, no redactions for relevance may be made within a produced Document or ESI item. Any redactions shall be clearly indicated on the face of the Document, with each redacted portion of the Document stating that it has been redacted and the basis for the redaction, and a metadata field shall indicate that the Document contains redactions and the basis for the redaction (e.g., "A/C Privilege"). Where a relevant Document contains both redacted and non-redacted content, Defendants shall produce the remainder of the non-redacted portions of the Document and the text/OCR corresponding to the non-redacted portions.

1. Spreadsheets. Spreadsheet files may be redacted in native format if redactions in non-native format are unduly burdensome or not reasonably feasible. Any Party electing to redact a spreadsheet in native format must make redactions clearly indicated on the face of the Document and upon request of the receiving Party, specify and explain what content was redacted if not readily apparent on the face of the redacted spreadsheet. The Parties must maintain an unaltered, unredacted version of the spreadsheet until the final disposition of the litigation, and nothing in this Order waives the right of either Party to challenge the

scope or permissibility of any redactions.

2. Other Documents. All Native Files that require redaction shall first be processed to show and reveal all non-redacted elements and formatting which are visible in the Native application, including but not limited to color, comments, revision marks, speaker notes, or other user-entered data which are visible in any view of the Document in its Native application, all of which shall be evident in the generated TIFF image(s). Redacted versions of Documents that contain color in their un-redacted form shall be produced in color in TIFF format when the color is necessary to understand the content, context, or meaning of the Document. Where reasonably possible, any occurrences of date/time auto-field items, including in headers and footers, will be removed and replaced with the term AUTODATE to prevent the current date from being printed. Email header information (*e.g.*, date, subject line, etc.) should not be redacted unless it is independently privileged. The production of a Document in a redacted form does not affect Defendants' obligation to timely assert and substantiate the assertion of privilege over the content in a privilege log. Defendants shall honor reasonable requests for the production of particular redacted Documents in other formats where the TIFF image is not reasonably usable.

t. Load File Formats.

ESI will be produced with a standard Concordance (*.dat) Load File format and an image Load File that is in .OPT format. The Concordance (*.dat) Load File shall be provided with UTF-8 encoding.

1. Load File names should contain the volume name of the production Media.
2. Unless other delimiters are specified, any fielded data provided in a Load File should use Concordance default delimiters. A semicolon (;) should be used as multi-entry

separator.

3. Any delimited text file containing fielded data should contain in the first line a list of the fields provided in the order in which they are organized in the file.

u. Metadata to Be Produced.

The metadata fields detailed in Exhibit A and B should be produced in the Load File for each Document to the extent that such information is available or, in the case of metadata created during processing such as Bates numbers, created, at the time of collection and processing, except that if a field contains privileged information, that privileged information may be redacted and noted in a corresponding privilege log.[2]

v. Extracted Text and OCR.

Each Document, whether produced in Native or in TIFF format, and whether originally existing in electronic or in hard copy, shall be produced with extracted text or OCR, as described herein.

1. Extracted Text (Emails, Unredacted Native ESI, and Redacted Spreadsheets). All email, un-redacted ESI, and redacted spreadsheets produced as Native files, should be provided with complete Document-level extracted text files. Full text shall be provided in the format of a single *.txt file for each file (i.e., not one *.txt file per *.tif image). Extracted text shall include all comments, revisions, tracked changes, speaker's notes and text from Documents with comments or tracked changes, and hidden and very hidden worksheets, slides, columns and rows. Text extracted from emails shall include all header information that

[2] The metadata fields listed in Exhibit A and B may be revised following the Parties' Rule 26(f) conference and subsequent consultations with technical experts to ensure proper collection and ingestion of metadata fields.

would be visible if the email was viewed in Outlook, including: (1) the individuals to whom the communication was directed ("To"), (2) the author of the email communication ("From"), (3) who was copied and blind copied on such email ("CC" and "BCC"), (4) the subject line of the email ("RE" or "Subject"), (5) the date and time of the email, and (6) the names of any attachments.

2. OCR (Redacted Native ESI, Documents). In the event a Document other than spreadsheets contains text that is to be redacted, Optical Character Recognition ("OCR") text files should be provided for any un-redacted portions of the Documents. Document-level OCR text files shall also be provided for all Hard Copy scanned Documents. OCR software must be set to the highest quality setting for any previously unscanned paper Documents, and reasonable quality control measures shall be used to ensure that the integrity of scanned copies of previously unscanned paper Documents are preserved for OCR (*e.g.*, pages are not angled or skewed or text is not blurred or obscured). Settings such as "auto-deskewing" and "auto-rotation" must be turned on during the OCR process to maximize text recognition on any given page.
3. Format of Extracted Text and OCR. The Extracted Full Text and/or OCR text for all deliverables should be in separate document-level, UTF-8 with BOM encoded TXT files provided in a separate folder. The number of TXT files per folder should be limited to 2,000 files.

w. Encryption.

To maximize the security of information in transit, any Media or file sharing Electronic Document repository on which Documents are produced must be encrypted by Defendants. Production deliverables provided via File Transfer Protocol ("FTP") shall be made available on a

secured FTP connection with AES 256-bit encryption. All production volumes uploaded by Defendants via this file sharing document repository shall remain available for download for no less than thirty calendar days. In such cases, the Defendants shall transmit the encryption key or password to a requesting Party, under separate cover, contemporaneously with sending the encrypted Media, or correspondence indicating the availability of the encrypted FTP deliverables.

12. CONTINUING OBLIGATIONS

The Parties will continue to meet and confer regarding any issues as necessary and appropriate. This Protocol does not address or resolve any objections to the scope of the Parties' respective discovery requests. The Parties agree that e-discovery will be conducted in phases, and the Parties will meet and confer regarding discovery of data sources not listed herein.

13. DOCUMENT STORAGE

During the pendency of this litigation, the Parties shall make reasonable efforts to preserve the originals of all Documents produced to the opposing Parties and to preserve the original Native format version of any ESI produced in non-Native format.

14. NO WAIVER

This Order shall not constitute a waiver of any objection to the ultimate discoverability, privilege, admissibility, or relevance of any records addressed herein.

15. GOOD FAITH COMPLIANCE AND CONFERRAL OBLIGATION

The Parties shall make good faith efforts to comply with and resolve any differences concerning compliance with this Order. No Party may seek relief from the Court concerning compliance with this Order unless it has first conferred with the other Parties. The Parties shall reasonably cooperate in the exchange of information concerning data systems and ESI as may be necessary to facilitate the discovery and exchange of ESI in these proceedings and to further the

exchange of information commenced at the Parties' Rule 26(f) conference.

16. NON-PARTY SUBPOENAS

A Party that issues a non-Party subpoena (the "Issuing Party") shall include a copy of this Order and a copy of the Stipulated Protective Order with such subpoena and state that the Parties in the litigation have requested that non-Parties produce Documents in accordance with the specifications set forth herein, including, specifically as to such non-Party productions:

The Issuing Party shall produce a copy to all other parties of any ESI (including any metadata) and Documents obtained by subpoena to a non-Party.

If the non-Party production is not Bates-stamped by the Non-Party Producer, prior to any Party reproducing the Non-Party Documents, the Parties will meet and confer to agree upon a format for designating the Documents with a unique Bates prefix and numbering scheme.

17. PRIVILEGE LOGS

a. The Parties will exchange privilege logs if any Documents are withheld by a producing Party on the basis of attorney-client privilege, the work-product doctrine, a joint-defense privilege, or any other applicable privilege, immunity, or prohibition on production. Privilege logs will be produced on a rolling basis within thirty days following the production from which the ESI or Document was withheld in whole or in part, subject to the parties' ability to extend such deadline by mutual agreement.

b. The Parties shall have no obligation to log work product or communications relating to this litigation, dating from February 9, 2023, prepared by or made with (1) counsel of record in the Litigation, or (2) in-house counsel. In addition, activities undertaken in compliance with the duty to preserve information (including, but not limited to, litigation hold letters) are protected from disclosure under Federal Rule of Civil Procedure 26(b)(3)(A) and (B),

and they need not be included on a privilege log unless they involve communications with a third Party not within the scope of the attorney-client privilege.

c. Where multiple individual email messages appear within a single email string, the Parties may include only a single privilege log entry, provided that such messages are contained in one individual email file, and each is subject to the same claim of privilege. The privilege log shall expressly identify if an entry contains multiple privileged communications that are not being separately logged. Any email metadata that appears on the privilege log shall be populated with the metadata from the top-level message. For the avoidance of doubt, this provision does not enable a party to avoid separately logging multiple documents on the basis that they reflect overlapping sub-parts of the same string (e.g., where the email chain is broken up or is produced multiple times from the perspective of different email participants).

d. Documents redacted for privilege are not required to be logged. Privilege redactions shall be clearly indicated on the face of the Document, with each redacted portion of the Document stating that it has been redacted and the basis for the redaction, and a metadata field shall indicate that the Document contains redactions and the basis for the redaction (e.g., "A/C Privilege").

e. If an email is produced with redactions, the redactions must not obscure the headers (from, to, cc, bcc, subject, sent date, of any embedded emails, unless the information redacted is independently privileged or otherwise protected.

f. If an email contains both privileged and non-privileged communications, the non-privileged communications must be produced, either by separately producing a copy of the non-privileged communications contained in the privileged communication, or by

producing a copy of the entire communication string with the privileged portions redacted

18. EFFECT OF ORDER

The Parties' agreement to this Order is without prejudice to the right of any Party to seek an order from the Court to rescind or amend this Order for good cause shown. Nothing in this Order shall abridge the rights of any person to seek judicial review or to pursue other appropriate judicial recourse with respect to any discovery ruling made by the Court in this matter.

19. NON-WAIVER AND CLAWBACK PROVISION

Pursuant to Federal Rule of Evidence 502(d), the production or disclosure of information containing material subject to a claim of attorney-client privilege or work product protection shall not constitute a waiver of the attorney-client privilege or work product protection applicable to such material, in this or any other proceeding, unless (a) the production or disclosure was made with the expressed intent by the producing Party to waive the attorney-client privilege or work product protection or (b) the producing Party making the production or disclosure has affirmatively used or relied on the specific material that is subject to the claim of attorney-client privilege or work product protection.

When a producing Party gives notice to a receiving Party that a Document or ESI subject to a claim of privilege or other protection has been inadvertently produced, the obligations of the receiving Party are those set forth in Federal Rule of Civil Procedure 26(b)(5)(B).

SO ORDERED, this 12th day November, 2024.

/s/
JULIE R. RUBIN
United States District Judge

EXHIBIT A

The chart below describes the metadata fields to be produced in generic, commonly used terms which the producing party is to adapt to the specific types of ESI it is producing, to the extent such metadata fields are included in the original electronic documents and can be customarily extracted as part of the electronic data discovery process. Any ambiguity about a metadata field is to be discussed with the receiving party prior to processing and production.

Field Name	Field Description
BegBates	Beginning document number
EndBates	Ending document number
BegAttach	Beginning document number of family unit
EndAttach	Ending document number of family unit
All Custodians	All names of people the document was collected from even if removed from production as a duplicate
Attachment Count	Number of attachments, same as Family Count
Author	Author field extracted from the metadata of the native file
From	Sender of the e-mail message
Recipient(s)	Recipient(s) of the e-mail message (To)
CC	Recipient(s) of "carbon copies" of the e-mail message
BCC	Recipient(s) of "blind carbon copies" of the e-mail message
Subject	Subject field extracted from the metadata of the native file
Sent Date	Date the e-mail message was sent (produced in "MM/DD/YYYY" format)
File Type	Mail, attachment, individual file
File Extension	File extension of document (.msg, .doc, .xls, etc.)
File Name	Name of original file
Title	Title of a non-email document (Microsoft Title field)
Hash Value	MD5 or SHA-1 Hash Value, unique document identifier
Nativelink	Relative file path to each native file on production media
Date Created	For non-emails (produced in "MM/DD/YYYY" format)
Redaction	Populate with Yes or No to indicate whether document contains redactions
Confidentiality	Populate with any confidentiality designation attached to the document
Source	The name of the producing party
Author	Author field extracted from the metadata of a non-email attachment
Custodian	Name of custodian or noncustodial source of document
Filepath	File/path of the location where the item was located at the time of collection
All File Paths	When global deduplication has been employed, all file paths to native files as they existed in original environment
ModifiedBy	Last user to modify non-email document as extracted from file system metadata or bib coding
ModifiedDate	The application recorded time on which a non-email document was last modified as
Redaction Reason	If the document contains redactions, the reason(s) for those redaction

EXHIBIT B

The chart below describes the metadata fields to be produced for Hardcopy Documents.

Field Name	Description of Field
BegBates	Beginning document number
EndBates	Ending document number
BegAttach	Beginning document number of family unit
EndAttach	Ending document number of family unit
All Custodians	All names of people the document was collected from even if removed from production as a duplicate
File Type	Mail, attachment, individual file
Redaction	Populate with Yes or No to indicate whether document contains redactions
Confidentiality	Populate with any confidentiality designation attached to the document
Source	The name of the producing party
Hardcopy	Indicates whether document is Hardcopy document that was scanned for production (Y/N)
Custodian	Name of custodian or noncustodial source of document
Redaction Reason	If the document contains redactions, the reason(s) for those redaction